MDS code

20^{th} January 2006

Theorem 1. Given a redundancy r and a minimum distance d. An $[n, n-r, d]$-code satisfies $d \leq r+1$.

§

Definition 1. A linear $[n, k, d]$ code over F with $d = n - k + 1$ is called a *maximum distance separable* (MDS) code.

In other words, an MDS is a $[n, n-r, r+1]$-code.

§

Theorem 2. Suppose $2 \leq r \leq q$. Let $a_1, \ldots, a_{q-1}$ be the non-zero elements of $GF(q)$. Then the matrix

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 & 0 & \cdots & 0 \\ a_1 & a_2 & \cdots & a_{q-1} & 0 & 1 & \cdots & 0 \\ a_1^2 & a_2^2 & \cdots & a_{q-1}^2 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & & \vdots & \ddots & \vdots \\ a_1^{r-1} & a_2^{r-1} & \cdots & a_{q-1}^{r-1} & 0 & & \cdots & 1 \end{bmatrix}$$

is the parity check matrix of an MDS $q+1, q+1-r, r+1$ code. Equivalently, the columns of H form a $(q+1)$-arc in $PG(r-1, q)$.

§

Theorem 3. Let C be a linear $[n, k, d]$ code over a field F of q elements, where q is a prime power with a parity check matrix H. Then C has a code word of weight $w \leq l$ if and only if l columns of H are linearly dependent.

§

Theorem 4. Let C be a linear $[n, k, d]$ code over F with a parity check matrix H. Then C is an MDS code if and only if every $n-k$ columns of H are linearly independent.

§

Theorem 5. If a linear $[n, k, d]$ code C is MDS, then so is its dual $C^{\perp}$.

§

Corollary 5[1]. Let C be an $[n, k, d]$ linear code over $F = GF(q)$. Then the following statements are equivalent.

a. C is MDS
b. Every k columns of a generator matrix G of C are linearly independent
c. Every $n-k$ columns of a parity check matrix H of C are linearly independent

§

Problem 1. Show that linear $[n, 1, n]$, $[n, n-1, 2]$ and $[n, n, 1]$ codes exist over any finite field F.

§

Definition 2. We call *trivial MDS codes* the $[n, 1, n]$, $[n, n-1, 2]$ and $[n, n, 1]$ codes.

§

Theorem 6. The only binary MDS codes are the trivial ones.

§

Definition 3. A square matrix is said to be *non-singular* if its columns are linearly independent. Given any matrix A, a $s \times s$ *square submatrix* of A is a $s \times s$ matrix consisting of the entries from some s rows and s column of A.

§

Theorem 7. Let C be an $[n, k, --]$ code with parity check matrix $H = (A \quad I_{n-k})$. Then C is an MDS code if and only if every square submatrix of A is non-singular.

§

Theorem 8. Let C be an $[n, k, --]$ code with generator matrix $G = (I_k \quad A)$. Then C is an MDS code if and only if every square submatrix of A is non-singular.

§

Theorem 9. Let C be an $[n, k, d]$ MDS code. Then any k symbols of the code words may be taken as message symbols.

§

Theorem 10. Let C be an $[n, k, d]$ code over $GF(q)$. Then C is an MDS code if and only if C has a minimum distance code word with non-zero entries in any d coordinates.

§

Corollary 10[1]. The number of code words of weight $n - k + 1$ in an $[n, k, d]$ MDS code over $GF(q)$ is

$$(q-1)\binom{n}{n-k+1}$$

§

Problem 2. Given k and q, find the largest value, $m(k, q)$, of n such that $[n, k, n - k + 1]$ MDS code exists over $GF(q)$.

§

Because of Theorem 5, Problem 2 is equivalent to Problem 3.

Problem 3. Given k and q, find the largest n for which there is a $k \times n$ matrix over $GF(q)$, every k columns of which are linearly independent.

§

Problem 4. Given a k-dimensional vector space V over $GF(q)$, what is the order of a largest subset of V every k vectors of which form a basis of the same?.

§

Theorem 11. For any prime power q, we have $m(2, q) = q + 1$.

§

Theorem 12.

$$m(k, q) = k + 1$$

for $q \leq k$.

§

Bibliography

Raymond Hill. *A first course in coding theory.* Clarendon, 1986

L R Vermani. *Elements of algebraic codng theory.* Chapman & Hall, 1996